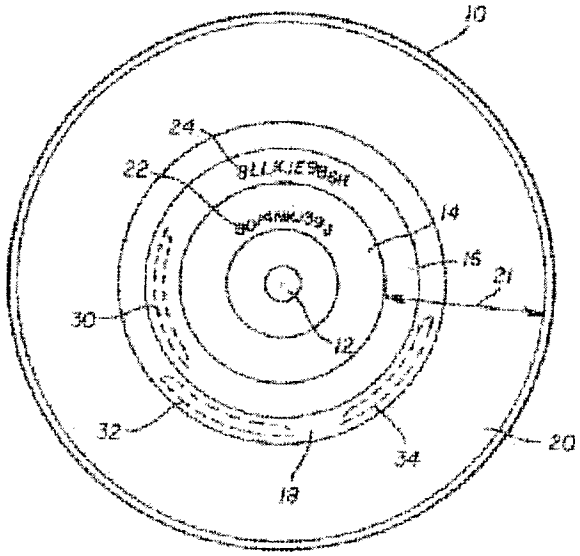
DELIVERY OF ELECTRONIC CONTENT OVER NETWORK USING HYBRID OPTICAL DISK FOR AUTHENTICATION

Publication number: JP2003115163 (A)
Publication date: 2003-04-18
Inventor(s): INCHALIK MICHAEL A; MUELLER WILLIAM J +
Applicant(s): EASTMAN KODAK CO +
Classification:
- international: ***G06F12/14; G06F1/00; G06F21/00; G06F21/24; G06Q50/00; G11B7/007; G11B7/30; G11B20/00; G11B20/10; G11B20/12; G11B27/00; H04N5/85; H04N7/167;*** **G06F12/14; G06F1/00; G06F21/00; G06Q50/00; G11B7/00; G11B7/007; G11B20/00; G11B20/10; G11B20/12; G11B27/00; H04N5/84; H04N7/167;** (IPC1-7): G11B20/10; G06F12/14; G06F17/60; G11B7/007; G11B7/30; G11B20/12; G11B27/00; H04N5/85; H04N7/167
- European: G11B20/00P; G06F21/00N5A2D; G06F21/00N7D; H04L9/08; H04L9/32
Application number: JP20020169245 20020610
Priority number(s): US20010878446 20010611

Also published as:
EP1267244 (A2)
US2003002671 (A1)
CN1391375 (A)

Abstract of **JP 2003115163 (A)**

PROBLEM TO BE SOLVED: To provide a legal user content which can be downloaded from a network such as the Internet and can also be used by a legal user at a plurality of places. SOLUTION: A method of transferring information from a database to a location that uses an authorizing hybrid disc, comprises the steps of: providing an authorizing hybrid optical disc having a ROM portion and a RAM portion; providing a ROM portion including a preformed identification signature; providing a RAM portion including user-specific encrypted information for providing a user-personalized secure signature in combination with the ROM preformed identification signature; a content supplier encrypting information for each user using the user-personalized secure signature and downloading selected encrypted information to a particular user's memory location; and using the user-personalized secure signature to decode the downloaded selected encrypted information.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－115163
（P2003－115163A）
(43)公開日　平成15年４月18日(2003.4.18)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ	20/10	Ｈ　５Ｂ０１７
					Ｄ　５Ｃ０５２
		３０１			３０１Ａ　５Ｃ０６４
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｅ　５Ｄ０４４
	17/60	１４２		17/60	１４２　５Ｄ０９０

審査請求　未請求　請求項の数３　ＯＬ　（全 22 頁）　最終頁に続く

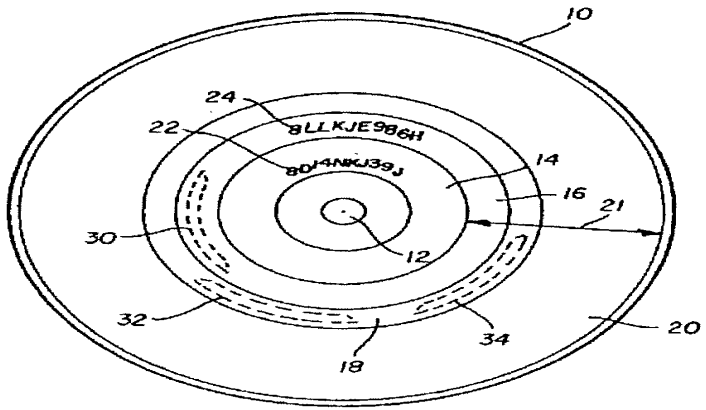
(21)出願番号　特願2002－169245(P2002－169245)
(22)出願日　平成14年６月10日(2002.6.10)
(31)優先権主張番号　８７８４４６
(32)優先日　平成13年６月11日(2001.6.11)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　590000846
イーストマン　コダック　カンパニー
アメリカ合衆国，ニューヨーク14650，ロチェスター，ステイト　ストリート343
(72)発明者　マイケル　アラン　インチャリック
アメリカ合衆国　ニューヨーク　14534
ピッツフォード　カッパーウッズ　30
(74)代理人　100070150
弁理士　伊東　忠彦　（外３名）

最終頁に続く

(54)【発明の名称】　認証のためのハイブリッド光ディスクを使用する、ネットワークを介した電子的コンテンツの配送

(57)【要約】
【課題】　本発明は、インターネットのようなネットワークからダウンロードでき且つ合法なユーザにより複数の場所で使用されることができる、合法なユーザにコンテンツを供給することを目的とする。
【解決手段】　認証するハイブリッドディスクを使用する位置へ、データベースから情報を転送する方法であって、ＲＯＭ部分とＲＡＭ部分とを有する認証するハイブリッド光ディスクを供給し、予め形成された確認署名を含むＲＯＭ部分を供給し、ＲＯＭの予め形成された確認署名と組合せてユーザの個人化安全署名を供給するユーザに特定の暗号化された情報を含むＲＡＭ部分を供給し、コンテンツ供給者がユーザに個人化された安全署名を使用して各ユーザに対して情報を暗号化し且つ選択された暗号化された情報を特定のユーザのメモリ位置へダウンロードし、ダウンロードされた選択された暗号化された情報を復号するためにユーザに個人化された安全署名を使用する方法。



【特許請求の範囲】
【請求項１】　そのような転送された情報の使用を許す認証するハイブリッドディスクを使用する位置へ、１つ又はそれ以上のデータベースから、コンテンツ供給者から、情報を転送する方法であって、その情報は、プログラム、オーディオ、静止画、ビデオ又は、データファイル（例えば、リスト、スプレッドシート、報告、ドキュメント、プレゼンテーショングラフィックス、販売情報）又は、それらの組合せを含み、
（ａ）ＲＯＭ部分とＲＡＭ部分とを有する、認証するハイブリッド光ディスクを供給するステップと、
（ｂ）ディスクのＲＯＭ部分内に刻印され、且つ、著作権侵害者がコピーすることが困難なように配置される、予め形成された確認署名を含むＲＯＭ部分を供給するステップと、
（ｃ）特定のユーザに対して光ディスクを唯一にし、且つ、ＲＯＭの予め形成された確認署名と組合せて、ユーザの個人化安全署名を供給する、ユーザに特定の暗号化された情報を含むＲＡＭ部分を供給するステップと、
（ｄ）コンテンツ供給者が、ユーザに個人化された安全署名を使用して、各ユーザに対して情報を暗号化し且つ、選択された暗号化された情報を特定のユーザのメモリ位置へダウンロードするステップと、
（ｅ）使用後に符号化された暗号化された情報のみがユーザのメモリ位置内に残るように、ユーザがそのような情報にアクセスしたいときには毎回、特定のユーザが、そのようにダウンロードされた選択された暗号化された情報を復号するために、ユーザに個人化された安全署名を使用するステップと、を有する方法。
【請求項２】　ハイブリッド光ディスクのＲＡＭ部分は、ダウンロードされるコンテンツに対するユーザメモリ位置である、請求項１に記載の方法。
【請求項３】　そのような転送された情報の使用を許す認証するハイブリッドディスクを使用する位置へ、１つ又はそれ以上のデータベースから、コンテンツ供給者から、情報の認証された転送を許す方法であって、その情報は、プログラム、オーディオ、静止画、ビデオ又は、データファイル（例えば、リスト、スプレッドシート、報告、ドキュメント、プレゼンテーショングラフィックス、販売情報）又は、それらの組合せを含み、
（ａ）ＲＯＭ部分とＲＡＭ部分とを有する、認証するハイブリッド光ディスクを供給するステップと、
（ｂ）ディスクのＲＯＭ部分内に刻印され、且つ、著作権侵害者がコピーすることが困難なように配置される、データベースからの情報を転送しかつ復号するための認証を許す、特定のユーザに唯一の予め形成された確認署名を含むＲＯＭ部分を供給するステップと、
（ｃ）特定のユーザに対して光ディスクを唯一にし、且つ、ＲＯＭの予め形成された確認署名と組合せて、ユーザの個人化安全署名を供給する、ユーザに特定の暗号化された情報を含むＲＡＭ部分を供給するステップと、
（ｄ）コンテンツ供給者に、認証するユーザに個人化された安全署名を供給し、且つ、ダウンロードされることが望まれる情報を選択することを、ユーザが、ネットワークを介してコンテンツ供給者と通信するステップと、
（ｅ）コンテンツ供給者が、ユーザに個人化された安全署名を使用して、暗号化し且つ、選択された暗号化された情報をユーザのメモリ位置へダウンロードするステップと、
（ｆ）使用後に符号化された暗号化された情報のみがユーザのメモリ位置内に残るように、ユーザがそのような情報にアクセスしたいときには毎回、ユーザが、そのようにダウンロードされた選択された暗号化された情報を復号するために、ユーザに個人化された安全署名を使用するステップと、を有する方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、遠隔位置から、安全な方法で、電子的コンテンツを配送することに関連する。
【０００２】
【従来の技術】大規模なコンピュータ化された装置の拡大で、従来は排他的に″ハードコピー″方法により共有されたデータの簡単で素早い共有が更に現実となってきている。これは、テキスト、音楽、静止画、ゲーム、ソフトウェア、ビデオ及び、他の形式の情報を含む。インターネットの広まった使用は、遠隔位置から全ての形式の情報をダウンロードすることをユーザに可能としている。これは、その特徴が、速度、顧客便利度、簡単な市場化及び、低コストを含む、新たな情報配布モデルを生成した。そのような作品の多くの物理的な生成が除去できるので、そのような作品を市場に出すのに、大きなコストと時間の節約が実現できる。大きな市場化の改善も実現できる。例えば、良くストックされた店は、今はキオスクのサイズであり又は、単一の位置に配置されそして、世界中でユーザにさらに便利である。
【０００３】これらのかなりの優位点と共に、配布の簡単さから、幾つかの欠点がある。これらの中の第１は、配布の簡単さは、作品の不法な拡散を許す。従来の本、オーディオ記録、又はビデオを、複製し且つ、他に配布するには、かなりの時間と努力を要するが、同じ作品の電子コピーを複製し且つ配布することは、簡単で、少しの時間と努力しか必要としない。これは、著者、芸術家、音楽家、プログラマー、プロデューサー、出版者及び、仕事が公共の領域でない者のかなりの懸念である。
【０００４】この問題は、認識され、そして、意図された受信者のみにより使用されるように、プログラムとデータを暗号化する幾つかの機構が開発された。幾つかの機構は、特定の鍵でデータを暗号化し、意図された受信者に、鍵を暗号化されたデータとともに送信することに

基づいている。しかしながら、受信者が、鍵を暗号化されたファイルと共有することを望む場合には、これらの機構は回避され得る。

【０００５】ＤｅＭｏｎｔの米国特許番号５，９８２，８８９は、情報製品に対するユーザのアクセスの真正を確認する方法を教示する。このシステムの欠点は、認証は、中央サイトを介してなされることである。製品を使用するたびに毎回ネットワークに接続したくない（又は、できない）ユーザは、製品を使用することから除かれる。

【０００６】Ａｋｉｙａｍａ他の米国特許番号５，８０５，６９９は、合法的な方法で、マスタ蓄積媒体内の記録されている著作権のあるソフトウェアをユーザの目標蓄積媒体にコピーすることを可能とする、ソフトウェアコピーシステムを提案する。マスタ蓄積媒体（即ち、ＣＤ－ＲＯＭ）はソフトウェア識別子を有し、そして、目標蓄積媒体は、蓄積媒体識別子を有する。２つの識別子は、ソフトウェア製品のコピーする権利にライセンスすることを管理する、中央サイトに送られる。中央サイトでは、コンピュータユーザに送り返される、第１の署名が２つの署名から発生される。ユーザのコンピュータでは、第２の署名が２つの同じ識別子から発生される。２つの署名が互いに一致するときのみ、ソフトウェアプログラムがマスタ蓄積媒体から目標蓄積媒体にコピーできる。

【０００７】これらの方法に関連する種々の問題がある。１つは、それらの多くは、″ハック（ｈａｃｋｓ）″として知られているものに開かれており、これは１人のユーザが、アプリケーション又はデータの復号又は使用する方法を決定すると、そのアプリケーション又はデータにアクセスする方法を広めることはその人にとって非常に簡単なことであることを意味する。幾つかの方法は、この問題を特定のハードウェアの組合せに依存する情報を使用することにより、避ける。このアプローチは、移植性の問題を発生する。合法なユーザは異なる位置で製品を使用することができないか又は、ユーザは、正しい使用を用いることができる（例えば、リセール、貸し出し）。ユーザが、彼らのハードウェア構成を、アップグレードのように、変更する場合には、アプリケーションは開始に失敗し、又は、データは読み出せない。

【０００８】

【発明が解決しようとする課題】従って、本発明の目的は、容易く、インターネットのようなネットワークからダウンロードでき、そして、合法なユーザにより複数の場所で使用されることができる、合法なユーザにコンテンツを供給することである。

【０００９】更に、本発明は、コンテンツが、不法なユーザによる秘密の情報の使用とアクセスに対して保護されることも目的とする。

【００１０】

【課題を解決するための手段】これらの目的は、そのような転送された情報の使用を許す認証するハイブリッドディスクを使用する位置へ、１つ又はそれ以上のデータベースから、コンテンツ供給者から、情報を転送する方法であって、その情報は、プログラム、オーディオ、静止画、ビデオ又は、データファイル（例えば、リスト、スプレッドシート、報告、ドキュメント、プレゼンテーショングラフィックス、販売情報）又は、それらの組合せを含み、（ａ）ＲＯＭ部分とＲＡＭ部分とを有する、認証するハイブリッド光ディスクを供給するステップと、（ｂ）ディスクのＲＯＭ部分内に刻印され、且つ、著作権侵害者がコピーすることが困難なように配置される、予め形成された確認署名を含むＲＯＭ部分を供給するステップと、（ｃ）特定のユーザに対して光ディスクを唯一にし、且つ、ＲＯＭの予め形成された確認署名と組合せて、ユーザの個人化安全署名を供給する、ユーザに特定の暗号化された情報を含むＲＡＭ部分を供給するステップと、（ｄ）コンテンツ供給者が、ユーザに個人化された安全署名を使用して、各ユーザに対して情報を暗号化し且つ、選択された暗号化された情報を特定のユーザのメモリ位置へダウンロードするステップと、（ｅ）使用後に符号化された暗号化された情報のみがユーザのメモリ位置内に残るように、ユーザがそのような情報にアクセスしたいときには毎回、特定のユーザが、そのようにダウンロードされた選択された暗号化された情報を復号するために、ユーザに個人化された安全署名を使用するステップと、を有する方法により達成される。

【００１１】コンテンツを伝送するための認証するハイブリッド光ディスクの使用は、コンテンツの供給者とユーザの両方に優位点がある。

【００１２】コンテンツ供給者は、インターネットのような、ネットワークを介してコンテンツを簡単に供給でき、これは、潜在的な世界中の聴衆に小さなオーバーヘッドを許す。ユーザに供給されるコンテンツは、そのユーザに″ロック″されることができ、それにより、認証されていないユーザは、認証されたユーザの認証するディスク無しでは、そのコンテンツを使用できない。供給者は、必要があるならば、この情報へのユーザアクセスを認証するディスクの使用を通して、秘密情報を供給提供できるがしかし、単一の認証するディスクを提供することも無しでは、ユーザはこれを他の者に配布できない。

【００１３】更に、ゲームのようなあるコンテンツが失われた又は盗まれた場合には、損失の元が追跡されることを可能とするために、ディスクに関連するコンテンツ内の個々の識別子は、元々″ロック″されていた。更なる安全な方法も、基本的な特徴に追加できる。

【００１４】ユーザへの優位点は、特定のユーザの認証

するディスクにロックされているという事実に関わらず、コンテンツは簡単に、インターネットのような、ネットワーク接続を介して生成されることを含む。コンテンツは、移植でき、ユーザが旅行中に持っていくと望む場合には、ユーザはコンテンツを（例えば、コンピュータのハードディスクに）コピーでき、そして、ディスクを持っていき、そして、ＣＤ－ＲＯＭドライブ、ＤＶＤリーダ等のような、光ディスクドライブを装備するどのコンピュータ上でも使用できる。更に、ユーザが光ディスクライターを有するならば、ユーザは、ユーザの認証するディスクに１つ以上のプログラム又はドキュメントをダウンロードすることができる。ディスクにコンテンツを書きこむ空間がある限り、ユーザは、追加のコンテンツを設置することができ、これをユーザは、単一のディスクへもっていくことが必要なのみで、使用できる。

【００１５】更なる優位点は、本発明は、ユーザへ、ユーザによる認証されていない配布からコンテンツの所有者を保護しながら正当な使用を行うことを許すことである。ユーザは、データ及び／又はソフトウェアのそれらのコピーを、貸し、再販し又は、与えることができるが、しかし、コンテンツの使用を許すために、それらの認証するディスクを、貸し／再販し／与えなけらばならない。ユーザは、単一のコピーのみの購入後に、複数のコピーの配布ができない。

【００１６】

【発明の実施の形態】図１は、認証するハイブリッド光ディスク１０を示す。認証するハイブリッド光ディスク１０は、ハイブリッド光ディスクであり、即ち、ＲＯＭ部分１４として知られるマスター化された予め記録された領域と、ＲＡＭ部分２１として知られる記録可能な領域の両方を有する。ディスクは、クランピングと回転のための中心穴１２を有する。ＲＯＭ部分１４は、マスター化されたセッションであり、即ち、マスターディスクは、第１セッションにソフトウェアとデータが供給され、そして、続いて、直接的に又は中間的な″父″及び″母″ディスクを通して、使用される、複数のカスタム化されていないディスクのコピーをスタンプするために、使用される。追加のマスター化セッションも可能である。ＲＡＭ部分２１は、ライトワンス形式（例えば、ＣＤ－ＷＯ又は、ＣＤ－Ｒ）又は、リライタブル形式（例えば、ＣＤ－ＲＷ）であり、標準的な光ディスク書き込み技術により、書き込みできる。認証するハイブリッド光ディスク１０も、予め形成された確認署名２２有し、これは、マスタリング処理中に記録されたディジタル信号であり、そして、続いて、認証するハイブリッド光ディスク１０のＲＯＭ部分１４に刻印される。予め形成された確認署名２２は、著作権侵害者がコピーするのが難しいように記録され、これは、上述の、Ｂａｒｎａｒｄ他により、２００１年１月２９日に出願された、名称″プログラマブルＣＤ－ＲＯＭ上の予め形成されたＩＤと唯一のＩＤを使用するコピー保護（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　Ｕｓｉｎｇ　ａ　Ｐｒｅｆｏｒｍｅｄ　ＩＤ　ａｎｄ　ａ　Ｕｎｉｑｕｅ　ＩＤｏｎ　ａ　Ｐｒｏｇｒａｍａｂｌｅ　ＣＤ－ＲＯＭ）″の、米国特許出願番号０９／７７２，３３３に開示されている。ＲＯＭ部分１４は、所定のアプリケーションの全てのディスクに共通な他の情報又はプログラムを含む。

【００１７】ＲＡＭ部分２１には、第２のセッション又は書き込みセッション１６が、コンテンツ供給者又は、他の認証されたパーティーにより、配布前に書きこまれる。コンテンツ供給者は、コピーしづらい方法でエンドユーザにコンテンツを入手できるようにするために、認証するハイブリッド光ディスク１０を使用したい、情報コンテンツ（例えば、オーディオ、ビデオ、テキスト、データ等）の製造、販売，再販に関係している人又は実体として定義される。コンテンツ供給者は、自分のデータベース内に情報コンテンツを維持し、そして、ネットワーク（例えば、インターネット）のようなネットワークを介してエンドユーザに情報を転送する。認証するハイブリッド光ディスク１０が既に１つ又はそれ以上のセッションを有する場合には、書き込みセッション１６が、第３又は、最後のセッションである。書き込みセッション１６は、暗号化された方法で、１つ又はそれ以上の既知の絶対セクターアドレスに書きこまれる、ユーザに特定の暗号化情報２４としても知られる、唯一の識別子番号又は、唯一のＩＤを有する。ユーザに特定の暗号化情報２４は、ハイブリッド光ディスク１０に書きこまれた各ユーザに特定の暗号化情報２４が唯一の組合せの２値のディジットであるということにより、各ハイブリッド光ディスク１０を特定のユーザに対して唯一にするように働く。ユーザに特定の暗号化情報２４は、ユーザに個人化された安全署名を構成するために、予め形成された確認署名２２と組合せられるようにも設計される。

【００１８】ある実施例では、書き込みセッション１６は、他のプログラム又は情報を有する。例えば、認証するハイブリッド光ディスク１０は、更に、暗号化されたクライアントアプリケーションパッケージ３０を含むことができ、これは、安全な方法で、認証するハイブリッド光ディスク１０の真正を確認するクライアントアプリケーションを含む。

【００１９】認証するハイブリッド光ディスク１０に関するマスタリングと製造の更なる詳細は、上述の、Ｈａ他による、１９９９年９月１０日に出願された、名称″コピー保護されたハイブリッド光記録ディスク（Ｈｙｂｒｉｄ　Ｏｐｔｉｃａｌ　Ｒｅｃｏｒｄｉｎｇ　Ｄｉｓｃ　ｗｉｔｈ　Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ）″の米国特許出願番号０９／３９３，５２７で教示され、その開示は参照によりここに組み込まれる。予め形成された確認署名２２とユーザに特定の暗号化情報２４の使用と要求に関する詳細は、上述の、Ｂａｒｎａｒｄ他によ

る、２００１年１月２９日に出願された、名称″プログラマブルＣＤ－ＲＯＭ上の予め形成あれたＩＤと唯一のＩＤを使用するコピー保護（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ Ｕｓｉｎｇ　ａ　Ｐｒｅｆｏｒｍｅｄ　ＩＤ　ａｎｄ　ａ　Ｕｎｉｑｕｅ　ＩＤｏｎ　ａ　Ｐｒｏｇｒａｍａｂｌｅ　ＣＤ－ＲＯＭ）″の米国特許出願番号０９／７７２，３３３で教示され、その開示は参照によりここに組み込まれる。

【００２０】認証するハイブリッド光ディスク１０は、ＣＤ－Ｒ、ＣＤ－ＷＯ、又は、ＣＤ－ＲＷライターのような、記録可能な光ディスク技術を使用して書きこまれる、１つ又はそれ以上の追加の書き込みセッション１８を有する。このセッションは、認証するハイブリッド光ディスク１０の配布後にいつでも書き込むことができ、そして、暗号化されたデータパッケージ３２と暗号化された実行可能パッケージ３４を含むことができる。認証するハイブリッド光ディスク１０は、更なる書き込み領域２０も含むことができ、それはＲＡＭ部分２１のまだ書きこまれていない部分である。

【００２１】用語″暗号化された方法で書きこむ″は、データがどのように蓄積されたかを知らないリーダーには、コンテンツが明らかでないように書きこまれることを意味する。図１ｂ、１ｃ及び、１ｄに戻ると、暗号化の幾つかの例示の方法の概略を示す。図１ｂは、唯一の識別子３５のシンボルが、個々の基準で又はブロックで、シンボル３６の他のシンボル又はグループで置き換えられる、置換機構を示す図である。図１ｃは、単純なハイディング（ｈｉｄｉｎｇ）機構を示し、そこでは、唯一の識別子３５が、シンボル３７の長い系列内に隠される。その位置と長さは、復号を行うために知らねばならない。図１ｄは、更に複雑なハイディング（ｈｉｄｉｎｇ）機構を示し、そこでは、唯一の識別子３５のシンボルは、個々に又はグループの何れかで、スクランブルされ、そして、シンボル３８の長い系列内に隠される。本発明は、ユーザに特定の暗号化情報２４を暗号化された方法で、認証するハイブリッド光ディスク１０のＲＡＭ部分２１に書きこむために、１つ又はそれ以上のこれらの機構又は、他の機構を使用できる。

【００２２】図２は、ユーザに個人化された安全署名を構成する方法を示す図である。予め形成された確認署名２２とユーザに特定の暗号化情報２４が連結され、ユーザに個人化された安全署名７２が構成される。

【００２３】次に図３は、暗号化されたクライントアプリケーションパッケージ３０が構成され、且つ、本発明で使用するために認証するハイブリッド光ディスク１０に書きこまれる１つの方法を示す図である。暗号化されたクライントアプリケーションパッケージ３０は、元の実行可能なプログラムとディスク上で同じ名前の単一の実行可能なプログラムである。暗号化されたクライントアプリケーションパッケージ３０は、最初に走る、自己抽出ソフトウェア４０を含む。さらに、プログラムが実行されたときメモリ内にハッキングソフトウェアの存在をチェックする、ハッキング対抗ルーチン４２を含む。さらに、多様なデータ及び／又はコマンド４４を有する部分のを含む。多様なコードは一般的には、同じ結果を達成する、複数の経路を提供するが、しかし、プログラムが実行されるときに毎回異なる経路を通るように構成される。多様なコードは、プログラムを更にリバースエンジニアリングしずらくするのに使用される。復号ルーチン４６は、暗号化されたクライアントアプリケーション５０復号するために、認証するハイブリッド光ディスク１０上に蓄積されたデータ（特に予め形成された確認署名２２とユーザに特定の暗号化情報２４）を使用するように設計される。暗号化されたクライントアプリケーションパッケージ３０は、さらに、公開鍵暗号化を使用して、安全な方法で、認証するハイブリッド光ディスク１０の真正と高潔さを確認するために使用される、秘密暗号鍵の組みを含む、秘密（プライベート）鍵領域５２を有する。

【００２４】図４は、本発明で使用される光ディスクを製造する方法のブロック図を示す。ハイブリッド光ディスクは、ステップ１１０で、予め形成された確認署名２２を用いてマスタ化され、そして、ステップ１１２で、同じ予め形成された確認署名２２を有する認証するハイブリッド光ディスク１０の組みを製造するために使用される。ディスクへの全ての連続する情報転送は、標準的なＣＤライター技術による。ステップ１１４で、個々の認証するハイブリッド光ディスク１０に対して、ユーザに特定の暗号化情報２４が発生される。予め形成された確認署名２２は、ディスクから読まれ（ステップ１１８）そして、ユーザに特定の暗号化情報２４と連結され、ユーザに個人化された安全署名７２を構成し、これは、暗号鍵としても働く（ステップ１２０）。ユーザに個人化された安全署名７２は、ステップ１２２で、クライアントアプリケーション６２を唯一に暗号化するのに使用される。暗号化されたクライアントアプリケーション５０は、ステップ１２４で、前に形成されたＩＳＯ９６６０互換のファイルイメージに挿入される。セッションの主データチャネルは、ユーザに特定の暗号化情報２４で修正され（ステップ１２６）、そして、全体のパッケージが、ステップ１２８で、ＲＡＭ部分１６として、認証するハイブリッド光ディスク１０に書きこまれる。これは、上述の、Ｂａｒｎａｒｄ他による、２００１年１月２９日に出願された、名称″プログラマブルＣＤ－ＲＯＭ上の予め形成あれたＩＤと唯一のＩＤを使用するコピー保護（Ｃｏｐｙ　Ｐｒｏｔｅｃｔｉｏｎ　Ｕｓｉｎｇ　ａ　Ｐｒｅｆｏｒｍｅｄ　ＩＤ　ａｎｄ　ａ　Ｕｎｉｑｕｅ　ＩＤ　ｏｎ　ａ　Ｐｒｏｇｒａｍａｂｌｅ　ＣＤ－ＲＯＭ）″の米国特許出願番号０９／７７２，３３３で詳細に開示される。認証するハイブリッド光デ

ィスク１０は、そして、多くの方法（例えば、メール、店を通した配布等）で配布される。

【００２５】図５ａは、認証するハイブリッド光ディスク１０の真正を確認し且つ続いて望まれるコンテンツを暗号化するために、ユーザに個人化された安全署名７２が、安全な方法で遠隔位置に送られる方法の概略を示す。これは、遠隔位置１７０により、認証するハイブリッド光ディスク１０の有効性を確認することを許す方法の使用を要求する。クライアントアプリケーション６２は、エンドユーザのコンピュータシステム上で走り、これは、物理的に遠隔位置１７０から離れているが、しかし、（例えば、インターネットのような）ネットワーク５８を介して接続されている。遠隔位置１７０は、望まれるコンテンツを暗号化し且つ送る方法を含む。クライアントアプリケーション６２は、これは、暗号化されたクライントアプリケーションパッケージ３０内で暗号化されたクライアントアプリケーション５０として、認証するハイブリッド光ディスク１０上で元々暗号化されており、データリードステップ７０で、認証するハイブリッド光ディスク１０から、予め形成された確認署名２２とユーザに特定の暗号化情報２４を読み、そして、それらをユーザに個人化された安全署名７２に結合するように設計されている。遠隔位置１７０は、ユーザに個人化された安全署名７２に関する鍵要求６４を、クライアントアプリケーション６２に送る。鍵要求６４に含まれているのは、要求に答えるときに、秘密鍵領域５２からの複数の鍵の１つを使用するメッセージである。クライアントアプリケーション６２は、ユーザに個人化された安全署名７２を、選択された秘密鍵で署名されている、署名されたメッセージ６６内で、遠隔位置１７０へ戻す。遠隔位置１７０は、選択した秘密鍵に対応する公開鍵を所有し、そして、クライアントアプリケーション６２の真正を確認でき、そして、従って、認証するハイブリッド光ディスク１０の真正を確認できる。遠隔位置１７０は、一旦ユーザに個人化された安全署名７２を所有すると、望まれるコンテンツを復号できる。これは、更に以下で詳しく述べる。

【００２６】図５ｂは、秘密鍵領域５２内で有効な秘密鍵、それらの対応する公開鍵と、それらが遠隔位置１７０とクライアントアプリケーション６２の間でどのように使用されるかの概略を示す。クライアントアプリケーション６２は、暗号化されたクライントアプリケーションパッケージ３０の秘密鍵領域５２内に蓄積された、秘密鍵シリーズ８０が設けられている。これらの秘密鍵は、対応する公開鍵で暗号化されたメッセージを復号できそして、それらは、安全な方法でメッセージに署名できる。例えば、秘密鍵８４（他の秘密鍵８６，８８，９０及び、９２も示されている）は、公開鍵９６で暗号化されたメッセージを復号できる（他の公開鍵９８，１００及び、１０２も示されている）。公開鍵９６は、秘密鍵８４により署名されたメッセージの真正をチェックできる。遠隔位置１７０は、秘密鍵シリーズ８０内の秘密鍵に対応する公開鍵の、公開鍵シリーズ８２を含む。公開鍵シリーズ８２は、秘密鍵シリーズ８０に対応する鍵の全体の組み又は、それのサブセットを有することができる。後者の配置は、クライアントアプリケーションを修正することなしに、１つのアプリケーション又は１つの供給者に対し、ある鍵を排他的に維持することを許す。何れかの鍵の安全性が傷つけられる場合には、特定の鍵が遠隔位置１７０から削除され、そして、安全性の傷が閉じられる。

【００２７】遠隔位置１７０は、ランダムに、公開鍵シリーズ８２から公開鍵″Ｘ″を選択し、それを選択された公開鍵１０６とする。遠隔位置１７０は、鍵要求６４をクライアントアプリケーション６２に送り、そして、どの鍵が選択された公開鍵１０６として選択されたかを鍵要求６４内で示す。クライアントアプリケーション６２は、秘密鍵シリーズ８０から対応する秘密鍵を選択し、選択された秘密鍵１０４を与える。選択された公開鍵１０６／選択された秘密鍵１０４の組みは、公開／秘密鍵チャネル１０８を構成する。クライアントアプリケーション６２は、遠隔位置１７０へ送られる署名されたメッセージ６６を署名するために、選択された秘密鍵１０４を使用する。

【００２８】図６ａは、ユーザが新たなコンテンツを要求したときに、発生するデータの流れを示す概略図である。このコンテンツは、プログラム、オーディオ、静止画、ビデオ又は、データファイル（例えば、リスト、スプレッドシート、報告、ドキュメント、プレゼンテーショングラフィックス、販売情報）又は、それらの組合せを含む。ユーザサイト１７１で、予め形成された確認署名２２とユーザに特定の暗号化情報２４が、ユーザに個人化された安全署名７２を構成するのに使用される。ユーザに個人化された安全署名７２は、ネットワーク５８を介して、遠隔位置１７０へ送られる。遠隔位置１７０では、ユーザにより注文された暗号化されていないコンテンツであるプレインコンテンツ７４は、ユーザに個人化された安全署名７２を使用して、暗号化ユーティリティ７６により、暗号化される。これは、選択された暗号化情報５６を形成する。プレインコンテンツ７４に依存して、選択された暗号化情報５６は、暗号化されたデータパッケージ３２又は、暗号化された実行可能パッケージ３４の何れかである。これらは、鍵としてユーザに個人化された安全署名７２で暗号化されているので、認証するハイブリッド光ディスク１０を所有するユーザは、選択された暗号化情報５６を使用することができる。選択された暗号化情報５６は、そして、ユーザサイト１７１にネットワーク５８を介してダウンロードされる。ユーザサイト１７１では、選択された暗号化情報５６は、メモリ位置７８に書きこまれる。この例では、メモリ位

置７８は、認証するハイブリッド光ディスク１０のＲＡＭ部分２１内の追加の書き込みセッション１８である。メモリ位置は、ディジタルコンテンツを蓄積できる他の位置（例えば、ハードドライブ、フレキシブルディスク、フラッシュＲＯＭ及び、その他）でも良い。

【００２９】ネットワークの性質は、複数のユーザが同時に、遠隔位置１７０にアクセスし、且つコンテンツをダウンロードすることを許すことは理解されよう。遠隔位置１７０は、各特定のユーザに対する、ユーザに個人化された安全署名７２を受信し、プレインコンテンツ７４を、特定のユーザのユーザに個人化された安全署名で暗号化し、選択された暗号化情報５６を特定のユーザのメモリ位置７８にダウンロードする。

【００３０】図６ｂは、ユーザに暗号化されたコンテンツを送るためのデータの代わりのフローを示す概略図である。この実施例では、ユーザに個人化された安全署名７２は、コンテンツ供給者の遠隔位置１７０でファイルされる。コンテンツに対する要求で、ユーザにより注文された暗号化されていないコンテンツである、プレインコンテンツ７４は、蓄積されたユーザに個人化された安全署名７２を使用して、暗号化ユーティリティ７６により暗号化される。これは、選択された暗号化情報５６を生成する。プレインコンテンツ７４の性質に依存して、選択された暗号化情報５６は、暗号化されたデータパッケージ３２又は、暗号化された実行可能パッケージ３４の何れかである。これらは、鍵として、ユーザに個人化された安全署名７２を使用して暗号化されているので、認証するハイブリッド光ディスク１０を所有するユーザは、選択された暗号化情報５６を使用することができる。選択された暗号化情報５６は、例えば、電子メールメッセージ７３を介して、登録されたユーザに送られることができる。この暗号化／配送方法は、ユーザ以外の者が（例えば、親類の買う贈り物）、所定のユーザのために、暗号化されたコンテンツを購入することを許す。安全性の考えから、コンテンツ供給者は、このサービスを含んでも含まなくても良い。

【００３１】図６ｃは、ディスクの所有者が、新たなコンテンツを得る方法を示す。ステップ１４０では、ユーザは、ネットワークを介して、コンテンツ供給者と通信する。ユーザは、家庭からインターネットサイトに接続でき、又は、このコンテンツを販売し且つ転送するキオスクのような、他の場所に行くことができる。ユーザがコンテンツ供給者と接続を達成する幾つかの手段がある。コンテンツ供給者の遠隔位置１７０は、チャネル（例えば、ネットワーク、インターネット等）を介してアクセス可能である。ユーザはコンテンツ供給者のアドレス（例えば、インターネットＵＲＬ）にタイプできる。代わりに、認証されたハイブリッド光ディスク１０は、自動的に又はリンク上のユーザクリックにより、ユーザを遠隔位置１７０に接続するリンクで符号化されることも可能である。後者の代わりは、ネットワークアドレスのタイプのユーザエラーの可能性を除去する。

【００３２】そして、ユーザは、ダウンロードしたいコンテンツを選択し（ステップ１４２）、そして、必要ならば、ネットワーク（例えば、インターネットを介してクレジットカード支払い）を介して通常の手段でコンテンツの支払いをする（ステップ１４４）。コンテンツは、ゲーム，音楽、ビデオ、本のようなテキスト、又は、他の形式のダウンロード可能な情報である。支払いは、ネットワークを介した支払いを行う通常の手段でも良い。ユーザは、ユーザの銀行又は他の商用機関からコンテンツ供給者へ所定の支払い額を認証する、支払い番号（例えば、デビット又は、クレジットカード番号）を、転送できる。（例えば、ユーザからの前納、コンテンツ供給者の送信の考え等により、）支払い番号が取る他の形式は、予め定められたダウンロードのユーザ番号を与える、コンテンツ供給者からの認証番号である。

【００３３】一旦ユーザが、望みのコンテンツを選択し且つ支払いをしたなら、ユーザは、認証するハイブリッド光ディスク１０をディスクライターに、ステップ１４６で置く。公にアクセス可能な、キオスクは、そのようなディスクライターを装備している。ユーザが家にいる場合には、メモリ位置７８が認証するハイブリッド光ディスク１０のＲＡＭ部分２１にある場合には、ユーザは、光ディスクライターを有しなければならい。クライアントアプリケーション６２は、自動開始又は、選択される（ステップ１４８）。クライアントアプリケーション６２は予め形成された確認署名２２とユーザに特定の暗号化情報２４を読み（ステップ１５０）、そして、それらをユーザに個人化された安全署名７２に連結し、これは、復号鍵として働く（ステップ１５２）。安全チャネルは、クライアントアプリケーション６２と遠隔位置１７０の間に確立され（ステップ１５４）そして、ユーザに個人化された安全署名７２は、遠隔位置１７０に供給される（ステップ１５６）。

【００３４】ステップ１５８では、遠隔位置１７０が、ユーザに個人化された安全署名７２は無効である決定する場合には、又は、失われた場合には、処理は停止する（ステップ１６０）。ユーザに個人化された安全署名７２は有効であると決定する場合には、伝送に対する認証は、許可されそして、遠隔位置１７０はプレインコンテンツ７４を、ユーザに個人化された安全署名７２を使用して、暗号化する（ステップ１６２）。（暗号化されたデータパッケージ３２又は暗号化された実行可能パッケージ３４で具体化される）暗号化情報５６は、ライターに送られ（ステップ１６４）、ここで、新たなセッションに書きこまれる（ステップ１６６）。ユーザは支払いを行い、そして、有効な認証するハイブリッド光ディスク１０を所有するとして確認されるので、これは、認証された転送として知られる。一旦コンテンツが完全に書

きこまれると、接触は閉じる（ステップ１６８）。

【００３５】図６ｄは、ユーザに個人化された安全署名７２を伝送する安全な方法の更なる詳細を示す。ステップ１７２で、遠隔位置１７０は、ランダムに、公開鍵シリーズ８２から、選択された公開鍵１０６を選択する。ステップ１７４では、遠隔位置１７０は、公開／秘密鍵チャネル１０８を使用するために、鍵要求６４をクライアントアプリケーション６２へ送る（即ち、ランダム鍵が選択される）。クライアントアプリケーション６２は、ユーザに個人化された安全署名７２を、メッセージにフォーマットし（ステップ１７６）、選択された秘密鍵１０４で署名する（ステップ１７８）。クライアントアプリケーション６２は、署名されたメッセージ６６を遠隔位置１７０へ送る（ステップ１８０）。遠隔位置１７０は、署名されたメッセージ６６受信しそして、署名されたメッセージ６６を確認するために選択された公開鍵１０６を使用する（ステップ１８２）。署名されたメッセージ６６が有効でない場合には（ステップ１８４）、処理は停止する（ステップ１８６）。署名されたメッセージ６６が有効な場合には、処理は継続する（ステップ１８８）。

【００３６】一旦ユーザが選択された暗号化情報５６を、認証された転送で、ダウンロードすると、認証するハイブリッド光ディスク１０は、ユーザが暗号化された情報にアクセスすることを許すように働く。暗号化情報５６は、（暗号化されたデータパッケージ３２として実現される）暗号化されたデータ又は、（暗号化された実行可能パッケージ３４として実現される）暗号化された実行可能なプログラムである。最初に、暗号化された実行可能なプログラムへのユーザアクセスを説明する。図７は、本発明で使用するために、暗号化された実行可能パッケージ３４が構造化されそして、認証するハイブリッド光ディスク１０に書きこまれる方法の図である。暗号化された実行可能パッケージ３４は、元の実行可能なプログラムとしてディスク上に同じ名前を有する、単一の実行可能なプログラムである。暗号化された実行可能パッケージ３４は、最初に走る自己抽出ソフトウェア４０を含む。更に、プログラムが実行されたときに、メモリ内にハッキングソフトウェアの存在をチェックする、ハッキング対抗ルーチン４２を有する。それは、更に、多様なデータ及び／又はコマンド４４を含む。多様なコードは一般的には、同じ結果を達成する、複数の経路を提供するが、しかし、プログラムが実行されるときに毎回異なる経路を通るように構成されそして、プログラムを更にリバースエンジニアリングしずらくする。復号ルーチン４６は、暗号化された実行可能４８を復号するために、認証するハイブリッド光ディスク１０上に蓄積されたデータ（特に予め形成された確認署名２２とユーザに特定の暗号化情報２４）を使用するように設計される。

【００３７】図８は、本発明が、エンドユーザの所有する、暗号化された実行可能パッケージ３４で動作するように設計される方法を示す。ステップ１９０では、エンドユーザは認証するハイブリッド光ディスク１０を、光ディスクドライブ（例えば、ＣＤ－ＲＯＭ，ＣＤ－Ｒ又は、ＣＤ－ＲＷドライブ）に挿入する。認証するハイブリッド光ディスク１０上の暗号化された実行可能パッケージ３４は、自動的に実行するか又は、選択される（ステップ１９２）。プログラムは最初に、プログラムをリバースエンジニアリングするのに使用され且つコピー保護機構を打ち負かす、ハッキングソフトウェアのチェックのために、ハッキング対抗ルーチン４２を使用する（ステップ１９４）。そのようなリバースエンジニアリングソフトウェアが存在する場合には、ハッキング対抗ルーチンは、ユーザにエラーメッセージを表示し、そして、自動的に停止する（ステップ１９６）。

【００３８】エンドユーザシステムに、リバースエンジニアリングソフトウェアが存在しない場合には、復号ルーチン４６は、予め形成された確認署名２２をステップ１９８で読む。ステップ２００では、復号ルーチン４６は、ユーザに特定の暗号化情報２４を認証するハイブリッド光ディスク１０から読む。ステップ２０２では、復号ルーチン４６は、ユーザに特定の暗号化情報２４と予め形成された確認署名２２を、ユーザに個人化された安全署名７２に連結し、これは暗号化鍵としても働く。ユーザに個人化された安全署名７２は、そして、暗号化された実行可能４８を復号するのに使用される（ステップ２０４）。プログラムはそして、暗号化が有効であったかを決定する（ステップ２０６）。これを行うのに、例えば、暗号化プログラム内のフラグを見つける又は、オペレーティングシステムに特有のコードが復号された実行可能に存在するかをチェックするように、幾つかの方法がある。復号が、不成功の場合には、エラーメッセージが表示され、そして、プログラム及び全体の処理が停止する（ステップ１９６）。復号が成功した場合には、元の実行可能は開始される（ステップ２０８）。

【００３９】復号ルーチン４６は、バックグランドに残り（ステップ２１２）、プログラムは実行し（ステップ２１０）そして終了する（ステップ２１４）。一旦もとのプログラムが、終了すると、復号ルーチン４６は、元のプログラムにより使用されるメモリとハードドライブ空間をクリアし（ステップ２１６）、そして、閉じる（ステップ２１８）。このように、元の実行可能の復号された形式は、削除されそして、符号化され暗号化された情報（例えば、暗号化された実行可能パッケージ３４）が、ユーザのメモリ位置７８内に残る。認証と復号処理は実行可能が開始されると毎回繰り返される。

【００４０】図９ａは、暗号化されたデータへのユーザアクセスを与える１つの方法を示す。この方法は、暗号化されたデータパッケージ３２を復号するために、復号

鍵を安全な方法で送る。暗号化されたデータパッケージ３２は、幾つかの方法で構成される。それは、全体の暗号化された情報よりなる。その場合には、暗号化された実行可能パッケージ３４にたいして使用されるサポーティングルーチン（例えば、自己抽出ソフトウェア４０、ハッキング対抗ルーチン４２）は、要求されない。暗号化されたデータパッケージ３２は、サポーティングルーチンを含むために構成されることができる。暗号化されたデータパッケージ３２は、示されているように又は、ハードドライブ、コンパクトフラッシュ（登録商標）等のような、ユーザシステム上の他のメモリ位置内に、認証するハイブリッド光ディスク１０上に蓄積され得る。

【００４１】安全な方法で互いに通信する２つのアプリケーションが、同じシステム上で使用される。第１は、再生アプリケーション又は、顧客アプリケーション６０であり、これは、暗号化されたデータパッケージ３２を復号するルーチンを含む、データ使用プログラム（例えば、テキストリーダ、スプレッドシート又はプレゼンテーションプログラム、サウンド又はビデオ再生アプリケーション）であるが、しかし、復号鍵は含んでいない。復号鍵は、第２のアプリケーションにより、それに渡される。第２のアプリケーションは、クライアントアプリケーション６２であり、それは、もともと、認証するハイブリッド光ディスク１０上で暗号化されている。クライアントアプリケーション６２は、データリードステップ７０で、認証するハイブリッド光ディスク１０から、予め形成された確認署名２２とユーザに特定の暗号化情報２４を、読みそして、それらを、暗号化鍵としても働くユーザに個人化された安全署名７２に結合するように設計される。顧客アプリケーション６０は、クライアントアプリケーション６２へ、ユーザに個人化された安全署名７２に関する最初に鍵要求６４を送る。鍵要求６４に含まれるのは、要求に答えるときに、秘密鍵領域５２からの複数の鍵の１つを使用するメッセージである。クライアントアプリケーション６０は、ユーザに個人化された安全署名７２を、選択された秘密鍵で署名されている、署名されたメッセージ６６内で、顧客アプリケーション６０へ戻す。顧客アプリケーション６０は、選択した秘密鍵に対応する公開鍵を所有し、そして、クライアントアプリケーション６２の真正を確認でき、そして、従って、認証するハイブリッド光ディスク１０の真正を確認できる。顧客アプリケーション６０は、一旦ユーザに個人化された安全署名７２を所有すると、認証するハイブリッド光ディスク１０から暗号化されたデータパッケージ３２を読むことができ（ステップ６８）、そして、それを復号できる。これは、更に以下で詳しく述べる。

【００４２】図９ｂは、秘密鍵領域５２内で有効な秘密鍵、それらの対応する公開鍵と、それらが顧客アプリケーション６０とクライアントアプリケーション６２の間でどのように使用されるかの概略を示す。図３を参照すると、クライアントアプリケーション６２は、暗号化されたクライントアプリケーションパッケージ３０の秘密鍵領域５２内に蓄積された、秘密鍵シリーズ８０が設けられている。これらの秘密鍵は、対応する公開鍵で暗号化されたメッセージを復号できそして、それらは、安全な方法でメッセージに署名できる。例えば、秘密鍵８４は、公開鍵９６で暗号化されたメッセージを復号できる。公開鍵９６は、秘密鍵８４により署名されたメッセージの真正をチェックできる。顧客アプリケーション６０は、秘密鍵シリーズ８０内の秘密鍵に対応する公開鍵の、公開鍵シリーズ８２を含む。公開鍵シリーズ８２は、秘密鍵シリーズ８０に対応する鍵の全体の組み又は、それのサブセットを有することができる。後者の配置は、クライアントアプリケーションを修正することなしに、１つのアプリケーション又は１つの供給者に対し、ある鍵を排他的に維持することを許す。何れかの鍵の安全性がが傷つけられる場合には、特定の鍵が顧客アプリケーション６０から削除され、そして、安全性の傷が閉じられる。

【００４３】顧客アプリケーション６０は、ランダムに、公開鍵シリーズ８２から公開鍵”Ｘ”を選択し、それを選択された公開鍵１０６とする。顧客アプリケーション６０は、鍵要求６４をクライアントアプリケーション６２に送り、そして、どの鍵が選択された公開鍵１０６として選択されたかを鍵要求６４内で示す。クライアントアプリケーション６２は、秘密鍵シリーズ８０から対応する秘密鍵を選択し、選択された秘密鍵１０４を与える。選択された公開鍵１０６／選択された秘密鍵１０４の組みは、公開／秘密鍵チャネル１０８を構成する。クライアントアプリケーション６２は、顧客アプリケーション６０へ送られる署名されたメッセージ６６を署名するために、選択された秘密鍵１０４を使用する。

【００４４】図１０、及び、図３、９ａ及び、９ｂを参照し、本発明は、選択された暗号化された情報を購入し且つダウンロードした特定のユーザの持つ、暗号化されたデータファイルと共に動作するように設計された、第１の実施例を示す。この実施例では、暗号化されたデータパッケージ３２は、認証するハイブリッド光ディスク１０上に蓄積されている。ステップ２２０で、ユーザは認証するハイブリッド光ディスク１０を光ディスクドライブに挿入する。顧客アプリケーション６０は、自動実行し又は、選択される（ステップ２２２）。ステップ２２４では、クライアントアプリケーション６２が、自動実行し又は開始される。顧客アプリケーション６０は、クライアントアプリケーション６２を開始するエージェント又は、要求者でもよい。クライアントアプリケーション６２は最初に、ホストマシン上で走るハッキングソフトウェアがあるかをチェックする（ステップ２２６）。そのようなソフトウェアは、クライアントアプリ

ケーション６２を壊そうとして、クライアントアプリケーション６２が使用するステップに続くように使用される。そのようなソフトウェアがホストマシン上で実行されている場合には、クライアントアプリケーション６２は停止し（ステップ２２８）そして、データの復号は可能ではない。

【００４５】ホストコンピュータが安全であると決定された場合には、クライアントアプリケーション６２は、ステップ２３０で、認証するハイブリッド光ディスク１０から、予め形成された確認署名２２とユーザに特定の暗号化情報２４を読み、そして、ステップ２３２で、２つのＩＤを、暗号化鍵としても働く、ユーザに個人化された安全署名７２に連結する。顧客アプリケーション６０は、ランダムに公開鍵シリーズ８２から選択された公開鍵１０６選択する（ステップ２３４）。ステップ２３６では、顧客アプリケーション６０は、クライアントアプリケーション６２へ、署名されたメッセージ６６で、ユーザに個人化された安全署名７２が送られることを要求する、鍵要求鍵要求６４を送る。クライアントアプリケーション６２は、ユーザに個人化された安全署名７２を含むメッセージを生成し、顧客アプリケーション６０により要求されるように選択された秘密鍵１０４でメッセージを署名し、そして、署名されたメッセージ６６を顧客アプリケーション６０に送る（ステップ２３８）。

【００４６】顧客アプリケーション６０は、署名されたメッセージ６６を受信しそして、ステップ２４０で、署名されたメッセージ６６の同一性を確認するために選択された公開鍵１０６を使用し、そして、認証するハイブリッド光ディスク１０の同一性を確認する。チェックが失敗すると、復号は停止し（ステップ２２８）そして、エンドユーザに復号されたコンテンツは示されない。おそらく、これは、ディスクが偽造又は、ある方法で損害を受けているためであろう。メッセージが有効である場合には、顧客アプリケーション６０は、ユーザに個人化された安全署名７２を使用し、ステップ２４２で、暗号化されたデータパッケージ３２を復号し、そして、それをエンドユーザに表示する（ステップ２４４）。

【００４７】図１１、及び、図３、９ａ及び、９ｂを参照し、本発明は、選択された暗号化された情報を購入し且つダウンロードした特定のユーザの持つ、暗号化されたデータファイルと共に動作するように設計された、第２の実施例を示す。この実施例では、暗号化されたデータパッケージ３２は、認証するハイブリッド光ディスク１０以外のメモリ位置（例えば、ユーザのハードドライブ）に蓄積されている。ステップ２５０、ユーザは、顧客アプリケーション１０（例えば、オーディオプレーヤ、ドキュメントビューア、プレゼンテーションプログラム）を選択する。ユーザ又は、アプリケーションは、ステップ２５２で、オープンするために、データファイルとして暗号化されたデータパッケージ３２を選択する。ステップ２５０と２５２は、オペレーティングシステムが対応するアプリケーションをオープンするデータファイルの選択を許す場合には、結合される。ステップ２５４では、顧客アプリケーション６０は、暗号化されたデータパッケージ３２は暗号化されたデータであることを認識する。顧客アプリケーション６０は、認証するハイブリッド光ディスク１０が挿入されねばならないというメッセージをユーザに表示する（ステップ２５６）。ステップ２５８で、ユーザは、認証するハイブリッド光ディスク１０を光ディスクに挿入する。ステップ２２４では、クライアントアプリケーション６２が、自動実行し又は開始される。顧客アプリケーション６０は、クライアントアプリケーション６２を開始するエージェント又は、要求者でもよい。クライアントアプリケーション６２は最初に、ホストマシン上で走るハッキングソフトウェアがあるかをチェックする（ステップ２２６）。そのようなソフトウェアは、クライアントアプリケーション６２を壊そうとして、クライアントアプリケーション６２が使用するステップに続くように使用される。そのようなソフトウェアがホストマシン上で実行されている場合には、クライアントアプリケーション６２は停止し（ステップ２２８）そして、データの復号は可能ではない。

【００４８】ホストコンピュータが安全であると決定された場合には、クライアントアプリケーション６２は、ステップ２３０で、認証するハイブリッド光ディスク１０から、予め形成された確認署名２２とユーザに特定の暗号化情報２４を読み、そして、ステップ２３２で、２つのＩＤを、暗号化鍵としても働く、ユーザに個人化された安全署名７２に連結する。顧客アプリケーション６０は、ランダムに公開鍵シリーズ８２から選択された公開鍵１０６選択する（ステップ２３４）。ステップ２３６では、顧客アプリケーション６０は、クライアントアプリケーション６２へ、署名されたメッセージ６６で、ユーザに個人化された安全署名７２が送られることを要求する、鍵要求鍵要求６４を送る。クライアントアプリケーション６２は、ユーザに個人化された安全署名７２を含むメッセージを生成し、顧客アプリケーション６０により要求されるように選択された秘密鍵１０４でメッセージを署名し、そして、署名されたメッセージ６６を顧客アプリケーション６０に送る（ステップ２３８）。

【００４９】顧客アプリケーション６０は、署名されたメッセージ６６を受信しそして、ステップ２４０で、署名されたメッセージ６６の同一性を確認するために選択された公開鍵１０６を使用し、そして、認証するハイブリッド光ディスク１０の同一性を確認する。チェックが失敗すると、復号は停止し（ステップ２２８）そして、エンドユーザに復号されたコンテンツは示されない。おそらく、これは、ディスクが偽造又は、ある方法で損害を受けているためであろう。メッセージが有効である場

合には、顧客アプリケーション６０は、ユーザに個人化された安全署名７２を使用し、ステップ２４２で、暗号化されたデータパッケージ３２を復号し、そして、それをエンドユーザに表示する（ステップ２４４）。

【００５０】本発明は、音楽、ビデオ、プライベートテキスト及び、写真及び、多くの、遠隔ダウンローディングをわたる高度な制御を許す。本発明とその遠隔ダウンローディングを亘る制御の程度は幾つかの例で最も良く示され得る、

例１。電子コンピュータゲームの製作者は、ゲームが顧客にダウンロード出来るようにすることを望む。これは、インターネットのようネットワーク５８を介して達成できる単純な配布モデルを形成する。しかしながら、ゲーム製作者は、エンドユーザを超えて配布することを制限したい。ゲーム製作者は、製造された認証するハイブリッド光ディスク１０を有することができる。各ディスクは、ＲＯＭ部分１４に刻印された（ディスクの組みに唯一である）予め形成された確認署名２２を含む。各ディスクは、唯一のユーザに特定の暗号化情報２４も含む。そのように準備されたディスクはゲーム製作者により、通常の配布手段（例えば、メール、ゲームプレーヤに訴える小売店、ゲーム雑誌のカバーに示され、等）で、顧客又は、潜在的な顧客へ、配布される。例えば、ディスクは、入手できる１つのゲームを購入するときに顧客にメールされ、そして、顧客が買う第１のゲームを含む。

【００５１】続くゲームに対して、ユーザは、単にゲーム製作者の、インターネット上のウェブサイトに接続し、望むゲームを注文するするだけで良い。ユーザは、電子的にゲームの支払いをする。ここで説明した技術を介して、ゲーム製作者は、望むゲームをユーザの認証するハイブリッド光ディスク１０の鍵に暗号化し、そして、暗号化されたゲームをユーザに送る。ユーザの位置では、ゲームは、（ユーザが光ディスクライターを有し、ユーザの認証するハイブリッド光ディスク１０に十分なスペースがあれば）認証するハイブリッド光ディスク１０に蓄積され、又は、ユーザのハードドライブのような他のメモリ位置に蓄積される。

【００５２】ゲームは、ユーザの認証するハイブリッド光ディスク１０が、ユーザのシステム上の光ディスクリーダー内で有効な場合にのみ実行するために、ここでで説明したのと同様な技術を使用できる、暗号化された実行可能ファイルである。

【００５３】このシナリオでは、ユーザは、ダウンロードされたゲームのコピーを作るのが自由である。例えば、ユーザは、旅行中にそれらにアクセスするために、幾つかのゲームをラップトップコンピュータに送りたい場合がある。これは、ユーザが認証するハイブリッド光ディスク１０をもって行く限り可能である。ユーザは、認証するハイブリッド光ディスク１０と共に、友達の家で実行するためにゲームを持っていくこともできる。しかしながら、永久に友達にゲームへのアクセスを与えるためには、ユーザは認証するハイブリッド光ディスク１０を移すことを必要とし、これは、そのディスクがアクセスを許していた全てのゲームへの自分自身のアクセスを取り除く。このように、ユーザは自由にゲームの正当な使用を行うことができ、しかし、ユーザによる配布から保護される。

【００５４】例２。電子ブック（しばしばｅ－ブックと呼ばれる）の″出版者″は、顧客に、ダウンロードで本を入手できるようにしたい。これは、インターネットのようネットワーク５８を介して達成できる単純な配布モデルを形成する。ゲームの場合のように、出版者は、エンドユーザを超えて配布することを制限したい。出版者は、製造された認証するハイブリッド光ディスク１０を有することができる。各ディスクは、ＲＯＭ部分１４に刻印された（ディスクの組みに唯一である）予め形成された確認署名２２を含む。各ディスクは、唯一のユーザに特定の暗号化情報２４も含む。そのように準備されたディスクは出版者により、通常の配布手段（例えば、メール、読者に訴える小売店、等）で、顧客又は、潜在的な顧客へ、配布される。例えば、ディスクは、入手できる１つのｅ－ブックを購入するときに顧客にメールされ、そして、顧客が買う第１のｅ－ブックを含む。

【００５５】続くｅ－ブックに対して、ユーザは、単に出版者の、インターネット上のウェブサイトに接続し、望むｅ－ブックを注文するするだけで良い。ユーザは、電子的にｅ－ブックの支払いをする。ここで説明した技術を介して、出版者は、望むｅ－ブックをユーザの認証するハイブリッド光ディスク１０の鍵に暗号化し、そして、暗号化されたｅ－ブックをユーザに送る。ユーザの位置では、ｅ－ブックは、（ユーザが光ディスクライターを有し、ユーザの認証するハイブリッド光ディスク１０に十分なスペースがあれば）認証するハイブリッド光ディスク１０に蓄積され、又は、ユーザのハードドライブのような他のメモリ位置に蓄積される。

【００５６】ｅ－ブックは、ユーザの認証するハイブリッド光ディスク１０が、ユーザのシステム上の光ディスクリーダー内で有効な場合にのみ、ここでで説明したのと同様な技術を使用して読まれることが可能な、暗号化されたデータファイルである。これは、クライアントアプリケーション６２を知っているテキストリーダの使用を必要とし、そして、暗号化されたデータを復号するために、ユーザに個人化された安全署名７２を使用する。出版者は、ユーザの最初の購入と共に、認証するハイブリッド光ディスク１０上にそのようなリーダーを含めることができる。

【００５７】このシナリオでは、ユーザは、ダウンロードされたｅ－ブックのコピーを作るのが自由である。例えば、ユーザは、旅行中にそれらにアクセスするため

に、幾つかのｅ－ブックをラップトップコンピュータに送りたい場合がある。これは、ユーザが認証するハイブリッド光ディスク１０をもって行く限り可能である。ユーザは、認証するハイブリッド光ディスク１０と共に、友達の家で実行するためにｅ－ブックを持っていくこともできる。しかしながら、永久に友達にｅ－ブックへのアクセスを与えるためには、ユーザは認証するハイブリッド光ディスク１０を移すことを必要とし、これは、そのディスクがアクセスを許していた全てのｅ－ブックへの自分自身のアクセスを取り除く。このように、ユーザは自由にｅ－ブックの正当な使用を行うことができ、しかし、ユーザによる配布から保護される。

【００５８】例３。中央研究所図書館は、幾つかの様々な会社位置でクリアランスを有する科学者に、ダウンロードで秘密報告を入手できるようにしたい。これは、会社のイントラネットのようネットワーク５８を介して達成できる単純な配布モデルを形成する。そのような報告の配布が、許可されたそれらの人にのみ厳しく制限されることは、会社の安全性には重要である。図書館は、製造された認証するハイブリッド光ディスク１０を有することができる。各ディスクは、ＲＯＭ部分１４に刻印された（ディスクの組みに唯一である）予め形成された確認署名２２を含む。各ディスクは、唯一のユーザに特定の暗号化情報２４も含む。そのように準備されたディスクは、会社の内部手段を介してへ、そのような配布の管理により許可された科学者に、配布される。

【００５９】報告を得るために、科学者は単に、イントラネット上の図書館のウェブサイトに接続し、必要な報告をダウンロードするだけで良い。図書館システムは、その科学者が、注文した報告へのクリアランスを有するかどうかを、認証するハイブリッド光ディスク１０から決定できる。ここで説明したの技術を介して、出版者は、報告をユーザの認証するハイブリッド光ディスク１０の鍵に暗号化し、そして、暗号化された報告を科学者に送る。科学者の位置では、報告は、（科学者が光ディスクライターを有し、認証するハイブリッド光ディスク１０に十分なスペースがあれば）認証するハイブリッド光ディスク１０に蓄積され、又は、科学者のハードドライブのような他のメモリ位置に蓄積される。

【００６０】報告は、科学者の認証するハイブリッド光ディスク１０が、科学者のシステム上の光ディスクリーダー内で有効な場合にのみ、ここでで説明したと同様な技術を使用して読まれることが可能な、暗号化されたデータファイルである。これは、クライアントアプリケーション６２を知っているテキストリーダの使用を必要とし、そして、暗号化されたデータを復号するために、ユーザに個人化された安全署名７２を使用する。図書館は、認証するハイブリッド光ディスク１０上にそのようなリーダーを含めることができる。

【００６１】このシナリオでは、科学者は、ダウンロードされた報告のコピーを作るのが自由である。例えば、科学者は、家でそれらを読みたい場合がある。これは、科学者が認証するハイブリッド光ディスク１０をもって行く限り可能である。しかしながら、特定の認証するハイブリッド光ディスク１０を所有しない者は、報告を、読むことができない。従って、科学者が、″鍵″ディスクで警告を行う限り、ファイルを見つけた者は、分類された会社情報を読むことができない。認証の複数の層と著作権侵害者検査手段は、認証するハイブリッド光ディスク１０の不法なコピーを誰もが簡単に作成できず、又は、アクセス情報を得るための他の方法を使用できず、そして、認証するハイブリッド光ディスク１０を模擬できない。このディスクは特定の科学者に鍵が付されているので、他の科学者に影響を与えること無く、失われたディスクに対して、アクセスはオフされることができる。

【００６２】

【発明の効果】本発明は、上述のように、容易く、インターネットのようなネットワークからダウンロードでき、そして、合法なユーザにより複数の場所で使用されることができる、合法なユーザにコンテンツを供給することができる。

【図面の簡単な説明】

【図１ａ】本発明に従ったコピー保護を許す認証されたハイブリッド光ディスクの平面図である。

【図１ｂ】暗号化の置換機構の概略を示す図である。

【図１ｃ】暗号化の単純なハイディング（ｈｉｄｉｎｇ）機構の概略を示す図である。

【図１ｄ】暗号化の更に複雑なハイディング機構の概略を示す図である。

【図２】安全署名を構成する方法を示す図である。

【図３】コピー可能でない方法でクライアントアプリケーションを暗号化するソフトウェア技術の概略を示す図である。

【図４】本発明で使用する光ディスクを作る方法の実施例のブロック図である。

【図５ａ】どのように、真正を確認するために、ネットワーク相互動作により、異なるコンピュータ上の種々のソフトウェアルーチンが接続されるかを示す概略図である。

【図５ｂ】暗号化に利用する公開鍵と、復号及びメッセージ署名に利用するその相補秘密鍵を示す概略図である。

【図６ａ】暗号化された情報を送るためのデータのフローを示す概略図である。

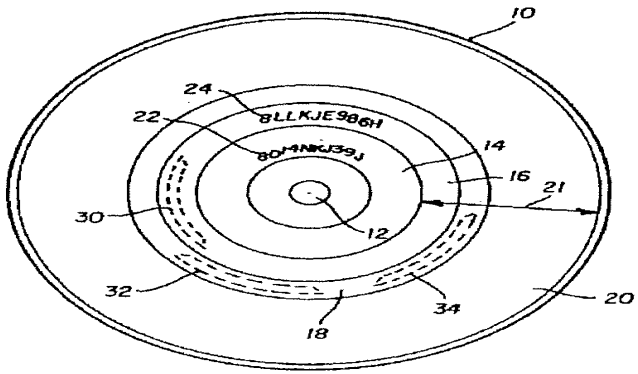
【図６ｂ】暗号化された情報を送るためのデータの代わりのフローを示す概略図である。

【図６ｃ】ディスクの所有者が新たなコンテンツを得る方法の実施例をを示すブロック図である。

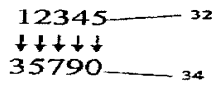
【図６ｄ】どのように、復号されたデータの復号内で、

通信のために、安全チャネルを形成するために、公開鍵と秘密鍵が使用されるかを示すブロック図である。
【図７】コピーできない方法で、暗号化されたデータを扱うために、実行可能なアプリケーションを暗号化するソフトウェア技術の概略を示す図である。
【図８】暗号化された実行可能なファイルを含むハイブリッド光ディスクが読まれたときに、どのようにコピー保護機構が動作するかを示すブロック図である。
【図９ａ】真正を確認しかつ暗号化されたデータを復号するために、どのように種々のソフトウェアルーチンが同じコンピュータ上で相互に動作するかを示す概略図である。
【図９ｂ】暗号化に利用する公開鍵と、復号及びメッセージ署名に利用するその相補秘密鍵を示す概略図である。
【図１０】暗号化されたデータファイルを含むハイブリッド光ディスクが読まれたときに、どのようにコピー保護機構が動作するかを示すブロック図である。
【図１１】本発明の他の実施例を示す図である。
【符号の説明】
１０　認証するハイブリッド光ディスク
１２　中心穴
１４　ＲＯＭ部分
１６　書き込みセッション
２０　書き込み領域
２１　ＲＡＭ部分
２２　予め形成された確認署名
２４　ユーザに特定の暗号化情報
３０　暗号化されたクライアントアプリケーションパッケージ
３０　暗号化されたクライントアプリケーションパッケージ
３２　暗号化されたデータパッケージ
３４　暗号化された実行可能パッケージ
３５　唯一の識別子
４０　自己抽出ソフトウェア
４２　ハッキング対抗ルーチン
４４　多様なデータ及び／又はコマンド
４６　復号ルーチン
５０　暗号化されたクライアントアプリケーション
５２　秘密鍵領域
５６　選択された暗号化情報
５８　ネットワーク
６０　顧客アプリケーション
６２　クライアントアプリケーション
６４　鍵要求
６６　署名されたメッセージ
７０　データリードステップ
７２　ユーザに個人化された安全署名
７３　電子メールメッセージ
７４　プレインコンテンツ
７６　暗号化ユーティリティ
７８　メモリ位置
８０　秘密鍵シリーズ
８２　公開鍵シリーズ
８４　秘密鍵
９６　公開鍵
１０４　選択された秘密鍵
１０６　選択された公開鍵
１０８　公開／秘密鍵チャネル
１７０　遠隔位置
１７１　ユーザサイト

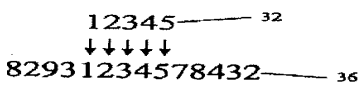
【図１ａ】



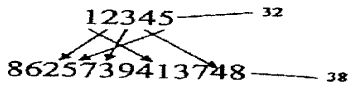
【図１ｂ】



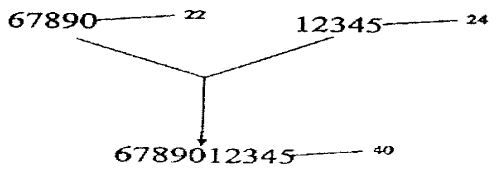
【図１ｃ】



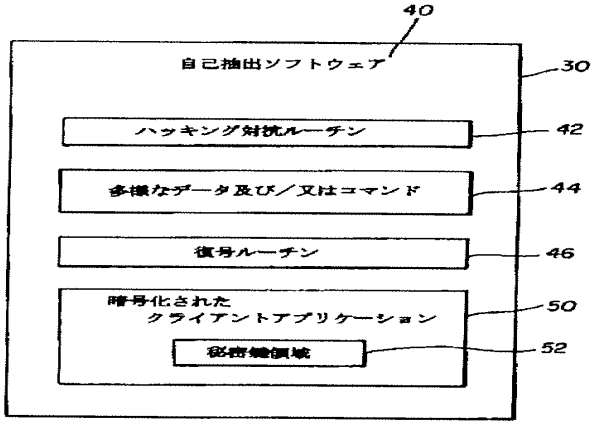
【図１ｄ】



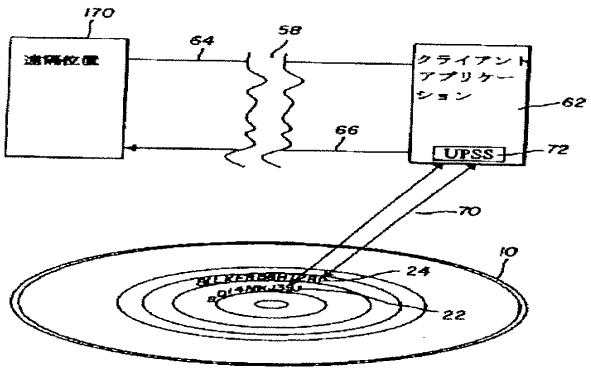
【図２】



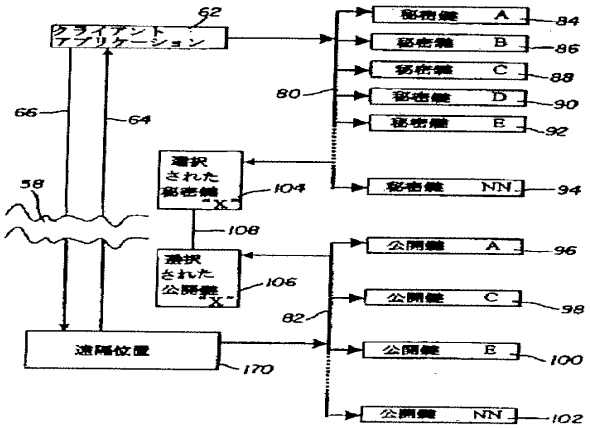
【図３】



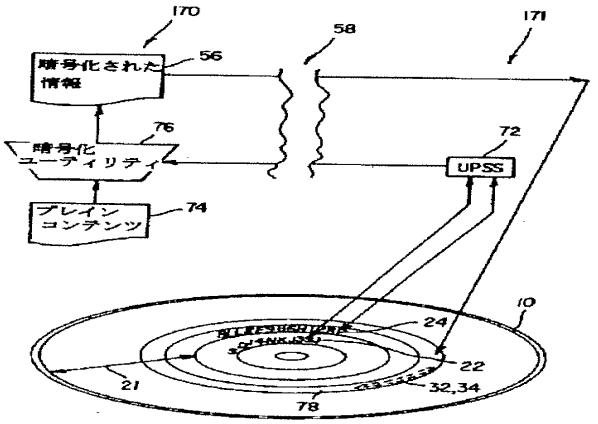
【図５ａ】



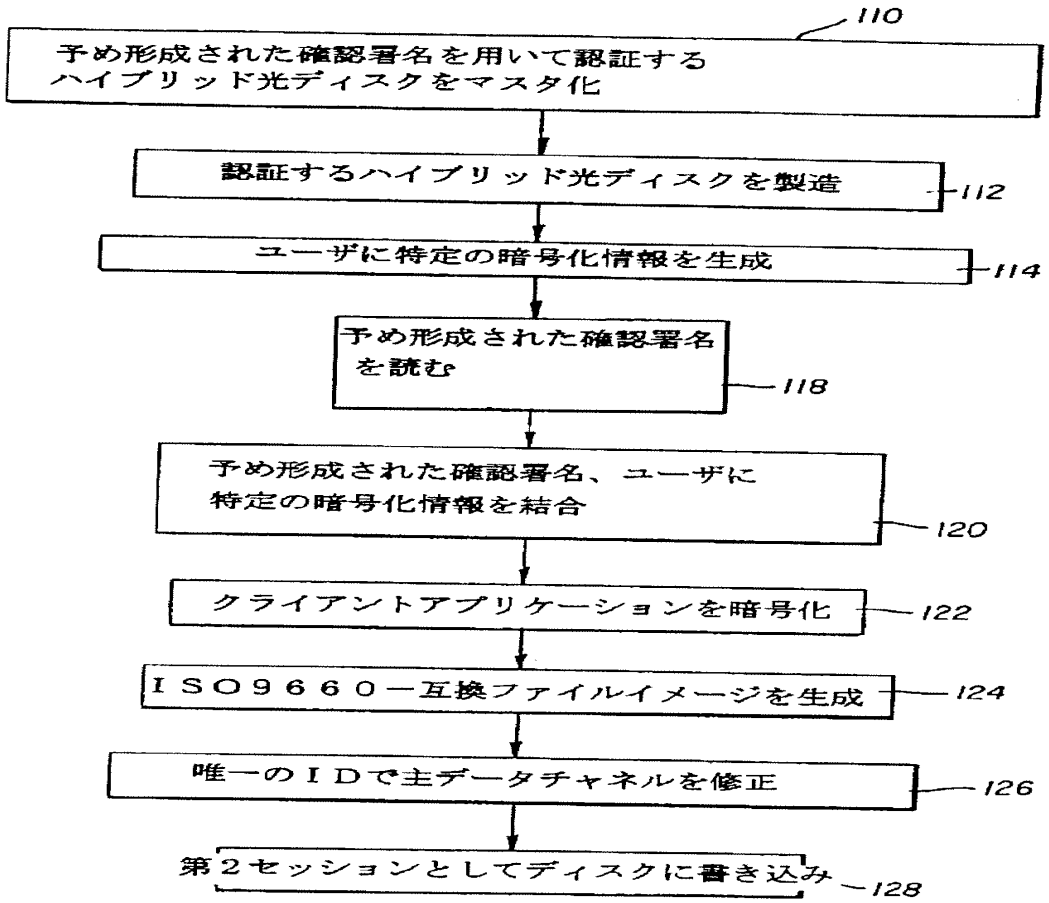
【図５ｂ】



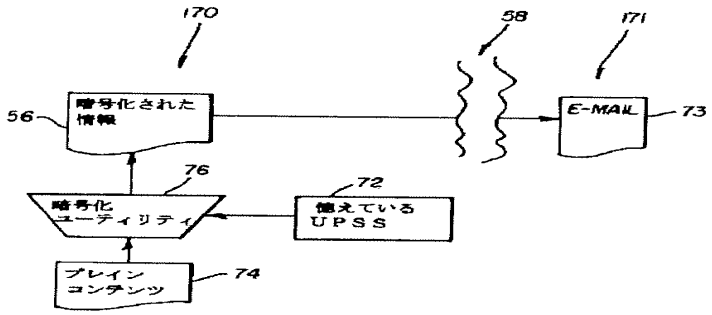
【図６ａ】



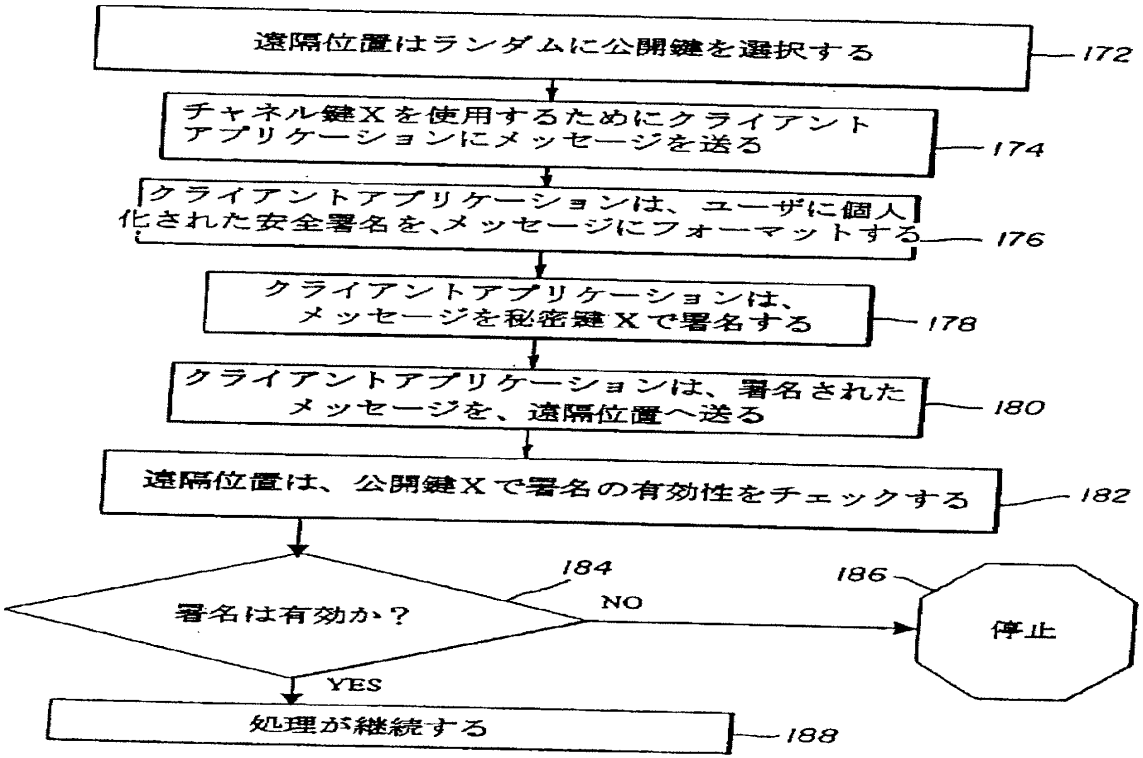
【図４】


110
予め形成された確認署名を用いて認証する
ハイブリッド光ディスクをマスタ化
認証するハイブリッド光ディスクを製造
112
ユーザに特定の暗号化情報を生成
114
予め形成された確認署名
を読む
118
予め形成された確認署名、ユーザに
特定の暗号化情報を結合
120
クライアントアプリケーションを暗号化
122
ＩＳＯ９６６０－互換ファイルイメージを生成
124
唯一のＩＤで主データチャネルを修正
126
第２セッションとしてディスクに書き込み
128

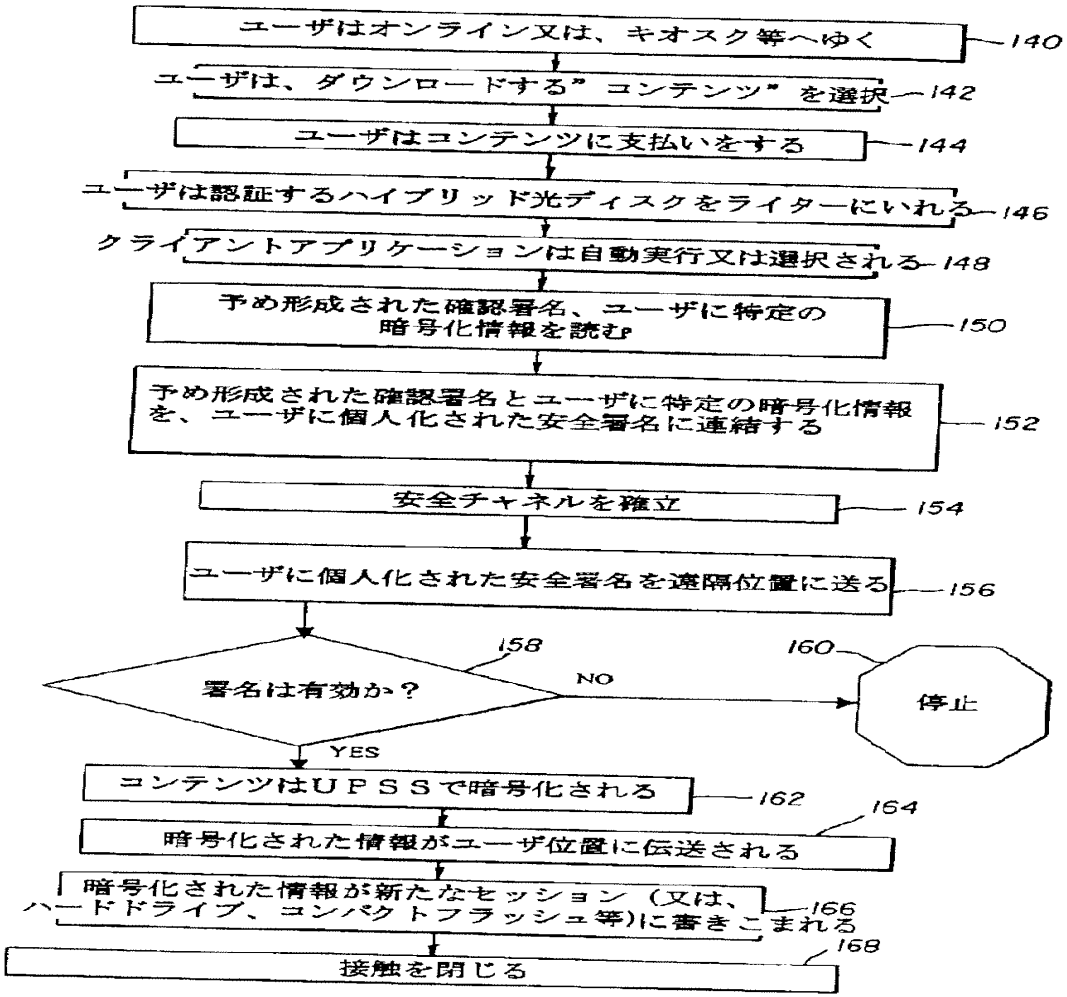
【図６ｂ】


170
58
171
暗号化された情報
56
E-MAIL
73
76
72
暗号化ユーティリティ
憶えているUPSS
ブレインコンテンツ
74

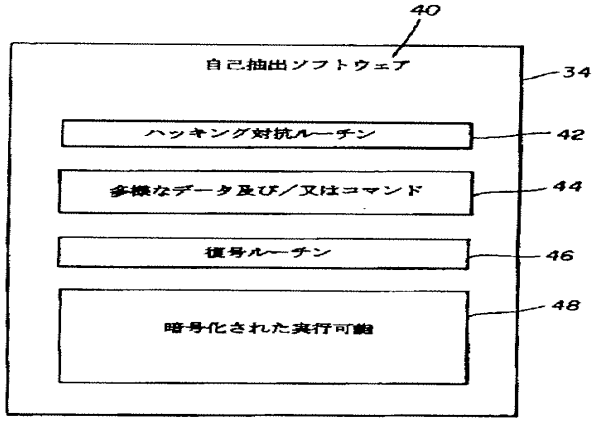
【図６ｄ】


遠隔位置はランダムに公開鍵を選択する
172
チャネル鍵Xを使用するためにクライアントアプリケーションにメッセージを送る
174
クライアントアプリケーションは、ユーザに個人化された安全署名を、メッセージにフォーマットする
176
クライアントアプリケーションは、メッセージを秘密鍵Xで署名する
178
クライアントアプリケーションは、署名されたメッセージを、遠隔位置へ送る
180
遠隔位置は、公開鍵Xで署名の有効性をチェックする
182
署名は有効か？
184
NO
186
停止
YES
処理が継続する
188

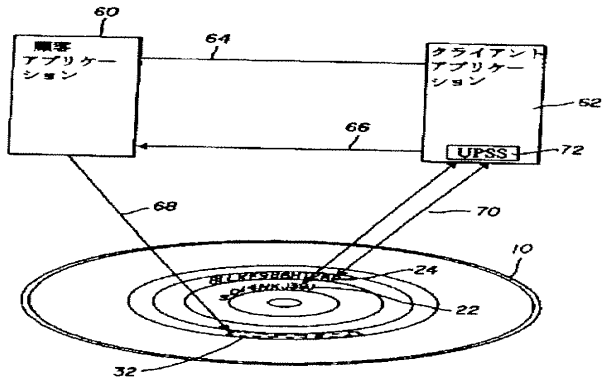
【図６ｃ】


ユーザはオンライン又は、キオスク等へゆく
140
ユーザは、ダウンロードする”コンテンツ”を選択
142
ユーザはコンテンツに支払いをする
144
ユーザは認証するハイブリッド光ディスクをライターにいれる
146
クライアントアプリケーションは自動実行又は選択される
148
予め形成された確認署名、ユーザに特定の暗号化情報を読む
150
予め形成された確認署名とユーザに特定の暗号化情報を、ユーザに個人化された安全署名に連結する
152
安全チャネルを確立
154
ユーザに個人化された安全署名を遠隔位置に送る
156
署名は有効か？
158
NO
160
停止
YES
コンテンツはＵＰＳＳで暗号化される
162
暗号化された情報がユーザ位置に伝送される
164
暗号化された情報が新たなセッション（又は、ハードドライブ、コンパクトフラッシュ等）に書きこまれる
166
接触を閉じる
168

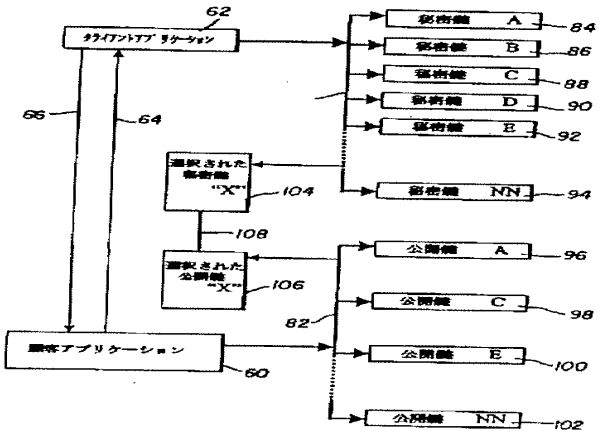
【図７】


40
自己抽出ソフトウェア
34
ハッキング対抗ルーチン
42
多様なデータ及び／又はコマンド
44
復号ルーチン
46
暗号化された実行可能
48

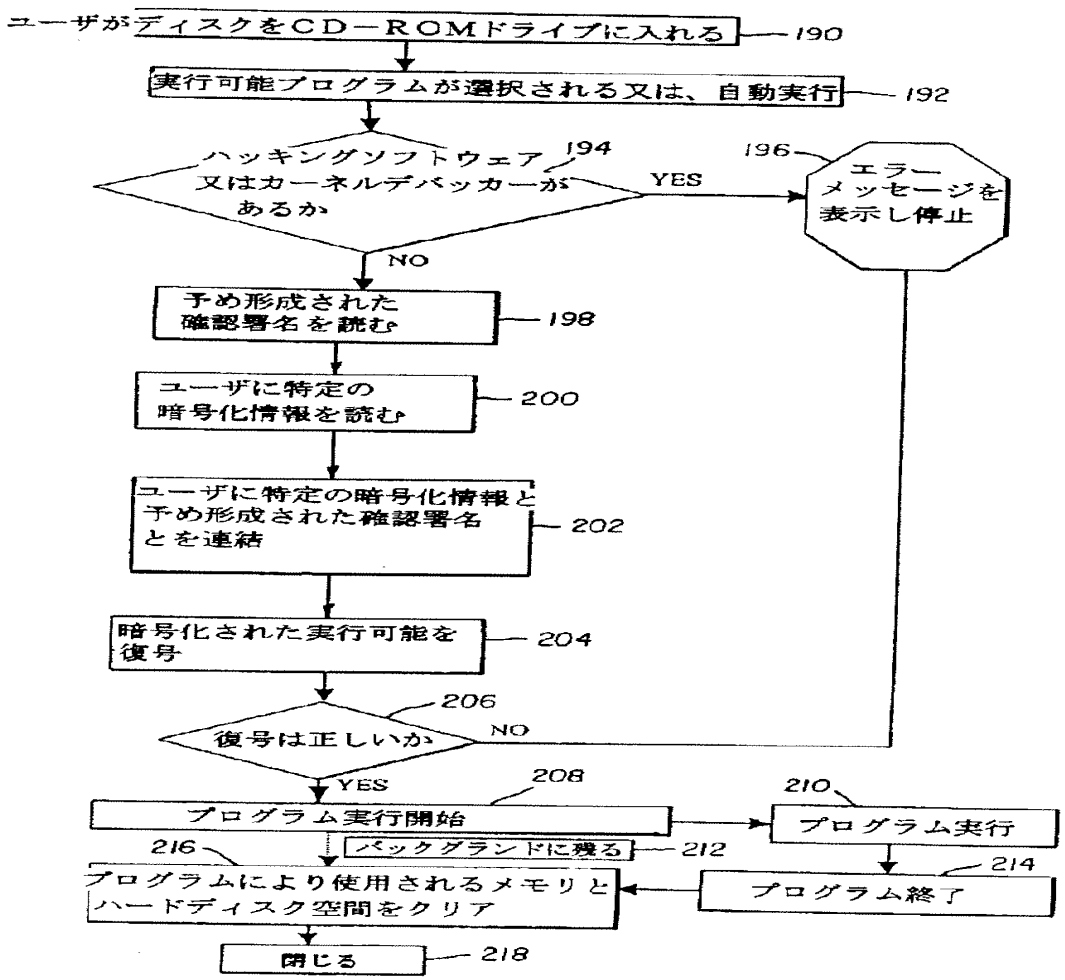
【図９ａ】


60
顧客アプリケーション
64
クライアントアプリケーション
62
66
UPSS
72
68
70
10
24
22
32

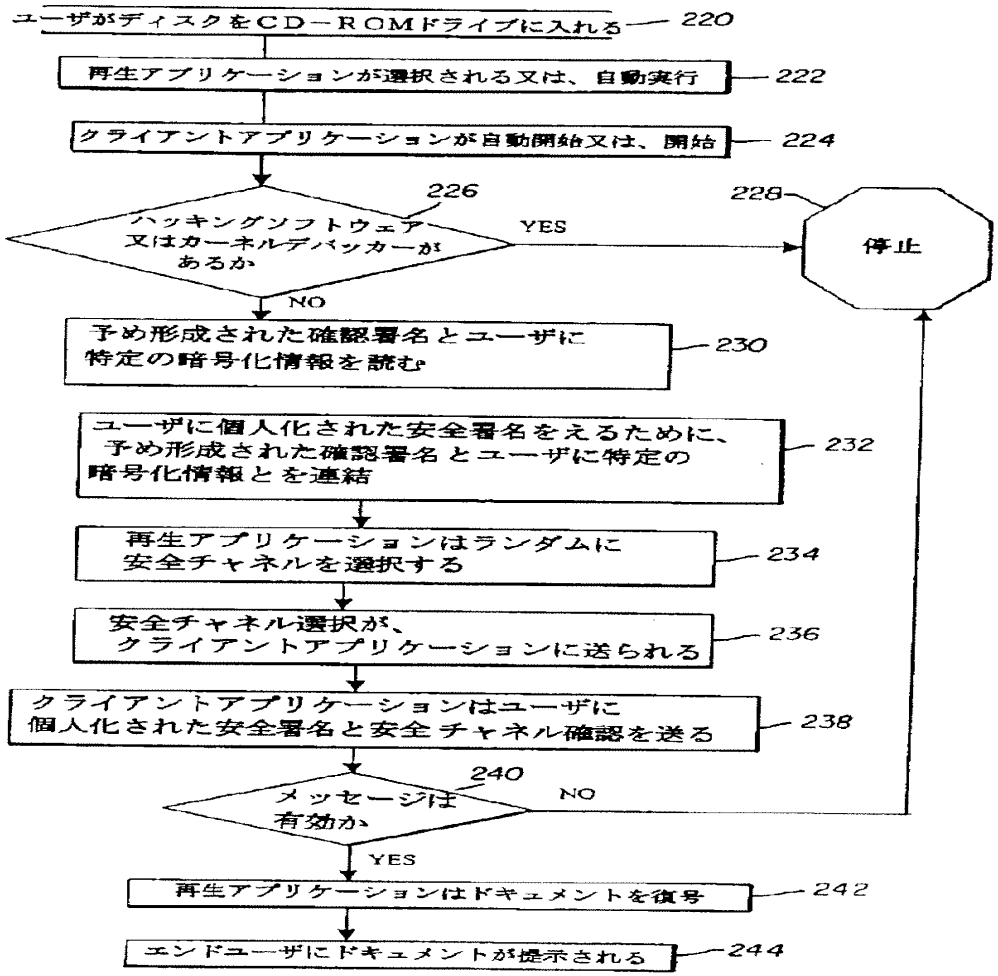
【図９ｂ】


62
クライアントアプリケーション
秘密鍵 A
84
秘密鍵 B
86
秘密鍵 C
88
秘密鍵 D
90
秘密鍵 E
92
66
64
選択された秘密鍵 "X"
104
秘密鍵 NN
94
108
選択された公開鍵 "X"
106
公開鍵 A
96
公開鍵 C
98
82
公開鍵 E
100
顧客アプリケーション
60
公開鍵 NN
102

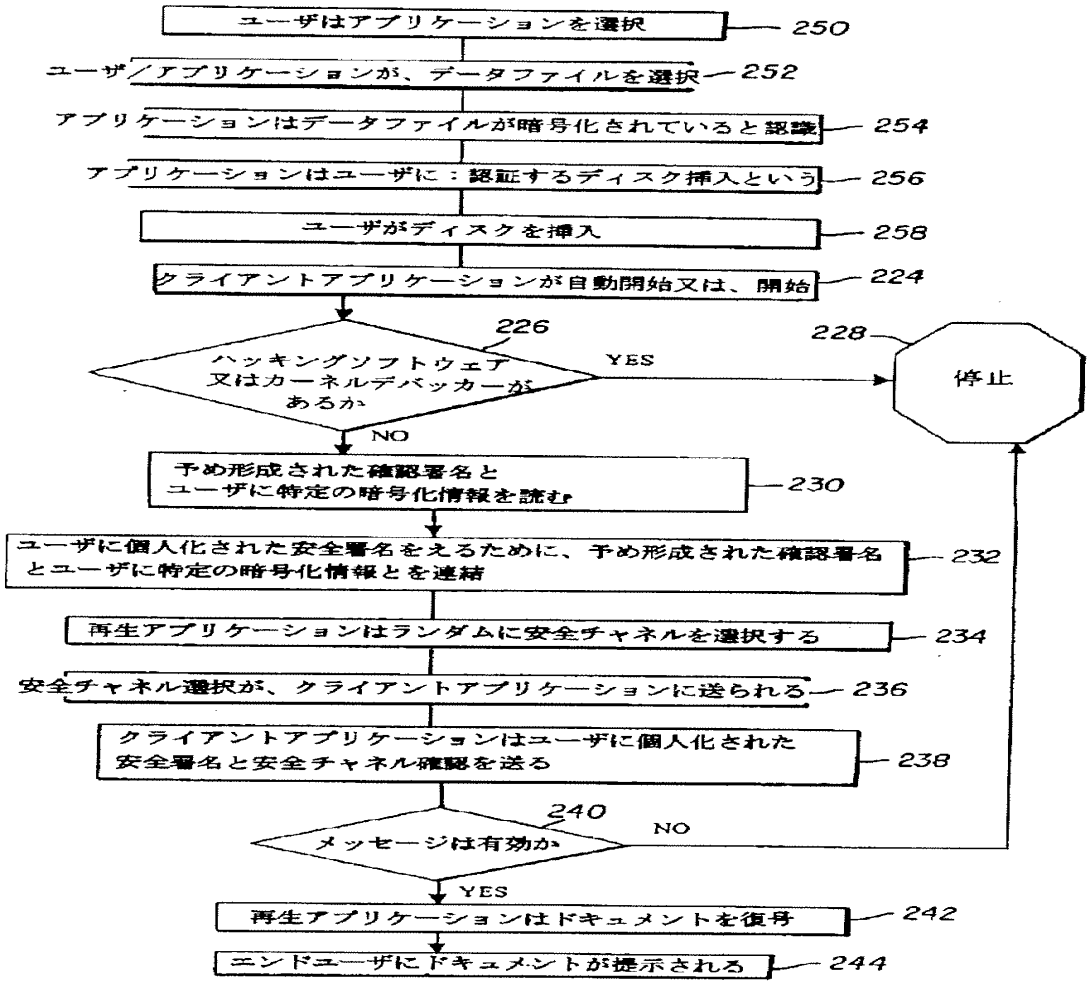
【図８】


ユーザがディスクをCD－ROMドライブに入れる
190
実行可能プログラムが選択される又は、自動実行
192
ハッキングソフトウェア又はカーネルデバッカーがあるか
194
YES
196
エラーメッセージを表示し停止
NO
予め形成された確認署名を読む
198
ユーザに特定の暗号化情報を読む
200
ユーザに特定の暗号化情報と予め形成された確認署名とを連結
202
暗号化された実行可能を復号
204
復号は正しいか
206
NO
YES
プログラム実行開始
208
プログラム実行
210
バックグランドに残る
212
プログラム終了
214
プログラムにより使用されるメモリとハードディスク空間をクリア
216
閉じる
218

【図１０】


ユーザがディスクをＣＤ－ＲＯＭドライブに入れる
220
再生アプリケーションが選択される又は、自動実行
222
クライアントアプリケーションが自動開始又は、開始
224
226
ハッキングソフトウェア又はカーネルデバッカーがあるか
YES
228
停止
NO
予め形成された確認署名とユーザに特定の暗号化情報を読む
230
ユーザに個人化された安全署名をえるために、予め形成された確認署名とユーザに特定の暗号化情報とを連結
232
再生アプリケーションはランダムに安全チャネルを選択する
234
安全チャネル選択が、クライアントアプリケーションに送られる
236
クライアントアプリケーションはユーザに個人化された安全署名と安全チャネル確認を送る
238
240
メッセージは有効か
NO
YES
再生アプリケーションはドキュメントを復号
242
エンドユーザにドキュメントが提示される
244

【図１１】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I		テーマコード（参考）
G１１B 7/007		G１１B 7/007		５D１１０
7/30		7/30	A	
20/12		20/12		
27/00		27/00	D	

Ｈ０４Ｎ　5/85
　　7/167

(72)発明者　ウィリアム　ジェイムズ　ミュラー
アメリカ合衆国　ニューヨーク　14586
ウエスト・ヘンリエッタ　アルヴァーストーン　ウェイ　53

Ｈ０４Ｎ　5/85　Ｚ
　　7/167　Ｚ

Ｆターム(参考)　5B017 AA03 AA06 BA07 CA09
5C052 AA02 AB03 AB04 AB08 AB09 DD02 DD04 DD06
5C064 BA01 BB02 BC06 BC22 BC25 CB08
5D044 AB02 AB05 AB07 BC04 BC06 CC06 DE02 DE03 DE12 DE49 DE50 DE54 DE57 DE58 GK12 GK17 HL08 HL11
5D090 AA01 BB04 CC01 CC14 FF09 HH01
5D110 AA17 AA18 AA27 AA29 BB25 BB27 BB29 DA08 DB03 DE04